# Senate

General Assembly

**File No. 705**

***January Session, 2015***

Substitute Senate Bill No. 949

*Senate, April 16, 2015*

The Committee on Government Administration and Elections reported through SEN. CASSANO, S. of the 4th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

***AN ACT IMPROVING DATA SECURITY AND AGENCY EFFECTIVENESS.***

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective July 1, 2015*) (a) As used in this section and section 2 of this act:

(1) "Contractor" means an individual, business or other entity that is receiving confidential information from a state contracting agency or agent of the state pursuant to a written agreement to perform services for the state.

(2) "State agency" means any agency with a department head, as defined in section 4-5 of the general statutes.

(3) "State contracting agency" means any state agency disclosing confidential information to a contractor pursuant to a written agreement with such contractor for the performance of services for the state.

(4) "Confidential information" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation. In addition, "confidential information" includes any information that a state agency identifies as confidential to the contractor. "Confidential information" does not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records that are lawfully made available to the general public.

(5) "Confidential information breach" means an instance where an unauthorized person or entity accesses or may have accessed confidential information in any manner, including, but not limited to, the following occurrences: (A) Any confidential information that is not encrypted or secured by any other method or technology that renders the personal information unreadable or unusable is misplaced, lost, stolen or in any way compromised; (B) one or more third parties have had access to, or taken control or possession of, without prior written authorization from the state, (i) any confidential information that is not encrypted or protected, or (ii) any encrypted or protected confidential information together with the confidential process or key that is capable of compromising the integrity of the confidential information; or (C) there is a substantial risk of identity theft or fraud of the client of the state contracting agency, the contractor, the state contracting agency or the state.

(b) Except as provided in section 2 of this act, every agreement that requires a state contracting agency to share confidential information with a contractor shall require the contractor to, at a minimum, do the

following:

(1) At its own expense, protect from a confidential information breach any and all confidential information that it comes to possess or control, wherever and however stored or maintained;

(2) Implement and maintain a comprehensive data-security program for the protection of confidential information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of confidential information as set forth in all applicable federal and state law and written policies of the state contained in the agreement. Such data-security program shall include, but not be limited to, the following: (A) A security policy for contractor employees related to the storage, access and transportation of data containing confidential information; (B) reasonable restrictions on access to records containing confidential information, including the area where such records are kept and secure passwords for electronically stored records; (C) a process for reviewing policies and security measures at least annually; and (D) an active and ongoing employee security awareness program that is mandatory for all employees who may have access to confidential information provided by the state contracting agency that, at a minimum, advises such employees of the confidentiality of the information, the safeguards required to protect the information and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law;

(3) Limit access to confidential information to authorized contractor employees and their authorized agents, for authorized purposes as necessary for the completion of the contracted services;

(4) Maintain all electronic data obtained from state contracting agencies: (A) In a secure server; (B) on secure drives; (C) behind multilevel firewall protections and monitored by intrusion detection software; and (D) in a manner where access is restricted to authorized employees and their authorized agents; and

(5) Enter into and maintain an appropriate confidentiality agreement with each employee and authorized agent who has access to confidential information.

(c) Except as specifically provided for in the agreement, a contractor shall not:

(1) Store data on stand-alone computer or notebook hard disks or portable storage devices such as external or removable hard drives, flash cards, flash drives, compact disks or digital video disks; or

(2) Copy, reproduce or transmit data except as necessary for the completion of the contracted services.

(d) All copies of data of any type, including, but not limited to, any modifications or additions to data that contain confidential information, are subject to the provisions of this section in the same manner as the original data.

(e) In the case of a confidential information breach or suspected confidential information breach a contractor shall:

(1) Notify the state contracting agency and the Attorney General as soon as practical, but not later than twenty-four hours after the contractor becomes aware of or has reason to believe that any confidential information that the contractor possesses or controls has been subject to a confidential information breach or suspected confidential information breach;

(2) Immediately cease all use of the data provided by the state contracting agency or developed internally by the contractor if so directed by the state contracting agency;

(3) Not later than three business days after the notification, submit to the office of the Attorney General and the state contracting agency either (A) a report detailing the breach, or (B) a report detailing why, upon further investigation, the contractor believes no breach has occurred; and

(4) Not later than six days after the notification, submit to the office of the Attorney General and the state contracting agency a plan to mitigate the effects of the breach and specifying the steps taken to ensure future breaches do not occur, except that no such plan is required of a contractor who has reported that no breach has occurred under subdivision (3) of this subsection.

(f) Based on the report and, if applicable, the plan provided, the state contracting agency shall decide, in its sole discretion, whether to permit any contractor who has been directed to cease use of data under subdivision (2) of subsection (e) of this section, to recommence use of the data or whether to cancel the agreement.

(g) The Attorney General may investigate any violation of this section. If the Attorney General finds that a contractor has violated or is violating any provision of this section, the Attorney General may bring a civil action in the superior court for the judicial district of Hartford under this section in the name of the state against such contractor.

(h) If the confidential information or personally identifiable information, as defined in 34 CFR 99.3, that has been subject to a confidential information breach consists of education records, the contractor may be subject to a five-year ban from receiving access to such information imposed by the Department of Education.

(i) The requirements of this section shall be in addition to the requirements of section 36a-701b of the general statutes, and nothing in this section shall be construed to supersede a contractor's obligations pursuant to the Health Insurance Portability and Accountability Act of 1996 P.L. 104-191 (HIPAA), the Family Educational Rights and Privacy Act of 1974, 20 USC 1232g, (FERPA) or any other applicable federal or state law.

Sec. 2. (NEW) (*Effective July 1, 2015*) The Secretary of the Office of Policy and Management, or the secretary's designee, may require additional protections or alternate measures of security assurance for

any requirement of section 1 of this act where the facts and circumstances warrant such additional requirement or alternate measure after taking into consideration, among other factors, (1) the type of confidential information being shared, (2) the amount of confidential information being shared, (3) the purpose for which the information is being shared, and (4) the types of services being contracted for.

Sec. 3. Section 4-66 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective from passage*):

The Secretary of the Office of Policy and Management shall have the following functions and powers:

(1) To keep on file information concerning the state's general accounts;

(2) **[**to**]** To furnish all accounting statements relating to the financial condition of the state as a whole, to the condition and operation of state funds, to appropriations, to reserves and to costs of operations;

(3) **[**to**]** To furnish such statements as and when they are required for administrative purposes and, at the end of each fiscal period, to prepare and publish such financial statements and data as will convey to the General Assembly the essential facts as to the financial condition, the revenues and expenditures and the costs of operations of the state government;

(4) **[**to**]** To furnish to the State Comptroller on or before the twentieth day of each month cumulative monthly statements of revenues and expenditures to the end of the last-completed month together with **[**(1)**]** (A) a statement of estimated revenue by source to the end of the fiscal year, at least in the same detail as appears in the budget act, and **[**(2)**]** (B) a statement of appropriation requirements of the state's General Fund to the end of the fiscal year itemized as far as practicable for each budgeted agency, including estimates of lapsing appropriations, unallocated lapsing balances and unallocated

appropriation requirements;

(5) [to] To transmit to the Office of Fiscal Analysis a copy of monthly position data and monthly bond project run;

(6) [to] To inquire into the operation of, and make or recommend improvement in, the methods employed in the preparation of the budget and the procedure followed in determining whether the funds expended by the departments, boards, commissions and institutions supported in whole or in part by the state are wisely, judiciously and economically expended and to submit such findings and recommendations to the General Assembly at each regular session, together with drafts of proposed legislation, if any;

(7) [to] To examine each department, state college, state hospital, state-aided hospital, reformatory and prison and each other institution or other agency supported in whole or in part by the state, except public schools, for the purpose of determining the effectiveness of its policies, management, internal organization and operating procedures and the character, amount, quality and cost of the service rendered by each such department, institution or agency;

(8) [to] To recommend, and to assist any such department, institution or agency to effect, improvements in organization, management methods and procedures and to report its findings and recommendations and submit drafts of proposed legislation, if any, to the General Assembly at each regular session;

(9) [to] To consider and devise ways and means whereby comprehensive plans and designs to meet the needs of the several departments and institutions with respect to physical plant and equipment and whereby financial plans and programs for the capital expenditures involved may be made in advance and to make or assist in making such plans;

(10) [to] To devise and prescribe the form of operating reports that shall be periodically required from the several departments, boards,

commissions, institutions and agencies supported in whole or in part by the state;

(11) [to] To require the several departments, boards, commissions, institutions and agencies to make such reports for such periods as said secretary may determine; and

(12) [to] To verify the correctness of, and to analyze, all such reports and to take such action as may be deemed necessary to remedy unsatisfactory conditions disclosed by such reports.

Sec. 4. (NEW) (*Effective July 1, 2015*) (a) For purposes of this section:

(1) "Data" means statistical or factual information that: (A) is reflected in a list, table, graph, chart, or other nonnarrative form that can be digitally transmitted or processed; (B) is regularly created and maintained by or on behalf of an executive agency; and (C) records a measurement, transaction or determination related to the mission of the executive agency or is provided to such agency by any third party as required by any provision of law. "Data" does not include return and return information, as defined in section 12-15 of the general statutes;

(2) "Executive agency" means any agency with a department head, as defined in section 4-5 of the general statutes, a constituent unit of higher education, as defined in section 10a-1 of the general statutes, or the Office of Higher Education, established by section 10a-1d of the general statutes; and

(3) "State agency" means any office, department, board, council, commission, institution, constituent unit of the state system of higher education, technical high school or other agency in the executive, legislative or judicial branch of state government.

(b) The Secretary of the Office of Policy and Management shall develop a program to access, link, analyze and share data maintained by executive agencies and to respond to queries from any state agency, and from any private entity or person that would otherwise require

access to data maintained by two or more executive agencies. The secretary shall give priority to queries that seek to measure outcomes for state-funded programs or that may facilitate the development of policies to promote the effective, efficient and best use of state resources.

(c) The secretary shall establish policies and procedures to:

(1) Review and respond to queries to ensure (A) a response is permitted under state and federal law; (B) the privacy and confidentiality of protected data can be assured; and (C) the query is based on sound research design principles; and

(2) Protect and ensure the security, privacy, confidentiality and administrative value of data collected and maintained by executive agencies.

(d) The secretary shall, in consultation with the Chief Information Officer, develop and implement a secure information technology solution to link data across executive agencies and to develop and implement a detailed data security and safeguarding plan for the data accessed or shared through such solution.

(e) The secretary shall request from, and execute a memorandum of agreement with, each executive agency detailing data-sharing between the agency and the Office of Policy and Management. Each such agreement shall authorize the Office of Policy and Management to act on behalf of the executive agency that is a party to such agreement for purposes of data access, matching and sharing and shall include provisions to ensure the proper use, security and confidentiality of the data shared. Any executive agency that is requested by the secretary to execute such an agreement shall comply with such request.

(f) The secretary shall notify the applicable executive agency when data within such agency's custody has been requested under subsection (b) of this section.

(g) The Office of Policy and Management shall be an authorized

representative of the Labor Commissioner or administrator of unemployment compensation under chapter 567 of the general statutes and shall receive upon request by the secretary any information in the Labor Commissioner's possession relating to employment records that may include, but need not be limited to: Employee name, Social Security number, current residential address, name and address of the employer, employer North American Industry Classification System code and wages.

(h) For the purposes of the Freedom of Information Act, as defined in section 1-200 of the general statutes, the Office of Policy and Management shall not be considered the agency with custody or control of any public records or files that are made accessible to said office pursuant to this section, but shall be considered the agency with custody and control of any public records or files created by the Office of Policy and Management, including, but not limited to, all reports generated by said office in response to queries posed under subsection (b) of this section.

| This act shall take effect as follows and shall amend the following sections: | | |
|---|---|---|
| Section 1 | *July 1, 2015* | New section |
| Sec. 2 | *July 1, 2015* | New section |
| Sec. 3 | *from passage* | 4-66 |
| Sec. 4 | *July 1, 2015* | New section |

***Statement of Legislative Commissioners:***
In Section 1(b)(4) "in a manner" was added for clarity, in Section 1(b)(5) "Require" was changed to "Enter into" for clarity and in Section 4(g) "is not" was changed to "need not be" for consistency.

***GAE*** *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

## *OFA Fiscal Note*

***State Impact:*** None

***Municipal Impact:*** None

### *Explanation*

The bill: 1) establishes protocols to protect certain confidential information handled by state contractors; and 2) allows the Office of Policy and Management (OPM) to develop a program to access, link, analyze, and share data maintained by executive agencies

The bill has no fiscal impact. The protocols regarding confidential information impact private businesses. Additionally, it is anticipated that OPM has the resources to develop the program required by the bill.

### *The Out Years*

***State Impact:*** None

***Municipal Impact:*** None

**OLR Bill Analysis**

**sSB 949**

***AN ACT IMPROVING DATA SECURITY AND AGENCY EFFECTIVENESS.***

**SUMMARY:**

This bill establishes protocols to protect confidential information (CI) that an entity obtains from a state contracting agency under a written agreement to perform services for the state. It also requires the Office of Policy and Management (OPM) secretary to develop a program to access, link, analyze, and share data maintained by executive agencies and respond to queries from state agencies and private requestors.

Under the bill, if an agreement requires a state contracting agency to share CI with a contractor, the contractor must, at its own expense, take certain steps to prevent data breaches. Among other things, contractors must, at a minimum:

1. implement and maintain a comprehensive data security program to protect the CI;

2. limit CI access to authorized employees and authorized agents for authorized purposes under confidential agreements;

3. maintain all data obtained from state contracting agencies using certain technology, such as firewalls and intrusion detection software, and may not maintain it using other technology such as removable hard drives and flash drives; and

4. report actual or suspected data breaches to the attorney general (AG) within 24 hours of the discovery.

With regard to the OPM data access program, the bill requires the

OPM secretary to:

1. establish policies and procedures to review and respond to queries while protecting the confidentiality of data,

2. develop and implement a secure information technology solution to link data across executive agencies, and

3. execute an agreement with each agency detailing data-sharing between the agency and OPM.

The bill's requirements for data security are in addition to others in existing law (see BACKGROUND). And the bill does not supersede contractors' obligations under the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), or any other applicable federal or state law.

The bill also makes technical changes pertaining to OPM's duties and responsibilities.

EFFECTIVE DATE: Upon passage for the technical provisions; July 1, 2015 for the remaining provisions.

## § 1 — CONFIDENTIAL INFORMATION

The bill defines "confidential information" as information that may be associated with a particular person through one or more identifiers. It includes:

1. the name, date of birth, and mother's maiden name;

2. any of the following numbers: motor vehicle operator's license, Social Security, employee identification, employer or taxpayer identification, alien registration, passport, health insurance identification, demand deposit or savings account, or credit or debit card;

3. unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation; and

4. any information that a state agency tells the contractor is confidential.

CI does not include information that may be lawfully obtained from public sources or federal, state, or local government records lawfully made available to the general public.

## § 1 — CONTRACTOR SECURITY PROTOCOLS

Except in cases where the OPM secretary grants a waiver (see below), every agreement that requires a state contracting agency to share CI with a contractor must require the contractor to, at a minimum, do the following:

1. at its own expense, protect from a CI breach any CI it possesses or controls, however stored or maintained;

2. implement and maintain a comprehensive data security program to protect CI;

3. limit CI access to authorized employees and their authorized agents for authorized purposes as necessary to complete contracted services;

4. maintain all data obtained from state contracting agencies (a) in a secure server, (b) on secure drives, (c) behind multilevel firewall protections and monitored by intrusion detection software, and (d) in a manner where access is restricted to authorized employees and authorized agents; and

5. enter into and maintain an appropriate confidentiality agreement with each employee and authorized agent who has CI access.

***Data Security Program.*** The safeguards contained in the contractor's required data security program (above) must be consistent with and comply with the safeguards for protecting confidential information, as set forth in all applicable federal and state laws and written policies of the state contained in the agreement. The program

must include the following, at a minimum:

1. a security policy for employees on storing, accessing, and transporting data containing CI;

2. reasonable restrictions on access to records containing CI, including the area where such records are kept, and secure passwords for electronically stored records;

3. a process for reviewing policies and security measures at least annually; and

4. a mandatory, active and ongoing employee security awareness program for all employees who have access to CI provided by the state contracting agency.

At a minimum, the security awareness program must advise the employees of the confidentiality of the information, safeguards required to protect the information, and any applicable state and federal civil and criminal penalties for noncompliance.

***Data Storage.*** Under the bill, contractors may not, unless specified in the agreement:

1. store data on stand-alone computer or notebook hard disks or portable storage devices such as external or removable hard drives, flash cards, flash drives, compact disks, or digital video disks or

2. copy, reproduce, or transmit data except as necessary to complete contracted services.

All copies of data, including modifications or additions that contain confidential information, are subject to the provisions governing the original data.

## § 1 — CI BREACHES

The bill defines "confidential information breach" as any instance where an unauthorized person or entity accesses or may have accessed

confidential information. This includes instances in which:

1. CI not encrypted or secured by any other method or technology that renders the personal information unreadable or unusable is misplaced, lost, stolen, or compromised;

2. a third party, without prior written state authorization, accesses or takes control or possession of (a) CI not encrypted or protected or (b) encrypted or protected CI and the confidential process or key capable of compromising its integrity; or

3. there is a substantial risk of identity theft or fraud of the client of the state contracting agency, contractor, state contracting agency, or state.

### *§ 1 — Notification of Data Breaches*

In the case of an actual or suspected CI breach, a contractor must:

1. notify the contracting agency and AG as soon as practical, but not later than 24 hours after becoming aware or having reason to believe that a breach has occurred;

2. immediately stop using the data provided by the contracting agency or developed internally by the contractor if the state contracting agency directs the contractor to do so; and

3. not later than three business days after the notification, submit to the AG's Office and the contracting agency either a report (a) detailing the breach or (b) explaining why, upon further investigation, the contractor believes no breach occurred; and

4. not later than six days after the notification, submit to the AG's Office and the contracting agency a plan to mitigate the effects of the breach and specifying steps taken to prevent future breaches. No plan is required from a contractor who reports that no breach occurred.

Based on the report and, if applicable, the plan submitted, the

contracting agency has sole discretion to decide whether to permit a contractor who was directed to stop using data to resume using the data or to cancel the agreement.

The AG may investigate and bring a civil action in Hartford Superior Court against contractors who have violated or are violating the provisions.

### *§ 1 — Breaches of Educational Records*

If the CI or personally identifiable information, as defined under federal law (34 CFR 99.3) that has been subject to a CI breach consists of education records, the contractor may be subject to a five-year ban from receiving access to such information, imposed by the Department of Education. The information in this case is:

1. a student's name or the name of the student's parent or other family members;

2. the address of the student or student's family;

3. a personal identifier, such as the student's birth, place of birth, or mother's maiden name;

4. **a** personal identifier, such as the student's Social Security number, student number, or biometric record;

5. other information that, alone or in combination, is linked or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

6. information requested by anyone who the educational agency or institution reasonably believes knows the identity of the student to whom the record relates.

The bill's provisions with regard to contractors must not be

construed to supersede a contractor's obligations under HIPAA, FERPA, or any other applicable federal or state law. (The HIPAA "privacy rule" sets national standards to protect the privacy of health information. It protects individually identifiable health information by defining and limiting the circumstances under which covered entities may use or disclose such information. Except under specified and limited circumstances, FERPA requires schools to obtain written permission from a parent or guardian before disclosing educational records to a third party.)

Also, the provisions are in addition to those on security data breaches in existing state law (CGS § 36a-701b—see BACKGROUND).

### *§ 2 — Additional Protections and Exceptions*

Under the bill, the OPM secretary, or his designee, may require additional protections or alternate security assurance measures for CI where the facts and circumstances warrant them after considering, among other factors, the:

1. type and amount of CI being shared,
2. purpose for which the CI is being shared, and
3. types of services covered by the contract.

### § 4 — OPM DATA ACCESS PROGRAM

The bill requires the OPM secretary to develop a program to access, link, analyze, and share data maintained by executive agencies and to respond to queries from state agencies, private entities, or others that would otherwise require access to data maintained by two or more executive agencies. The secretary must give priority to queries that seek to measure outcomes for state-funded programs or that may facilitate the development of policies to promote the effective, efficient, and best use of state resources.

Under the bill, (1) an "executive agency" is any agency with a department head, a constituent unit of higher education, and the Office

of Higher Education, and (2) "state agency" is any office; department; board; council; commission; institution; constituent unit of the state system of higher education; technical high school; or other executive, legislative or judicial branch agency.

"Data" means statistical or factual information that (1) is reflected in a list, table, graph, chart, or other nonnarrative form that can be digitally transmitted or processed; (2) is regularly created and maintained by or on behalf of an executive agency; and (3) records a measurement, transaction, or determination related to the mission of the executive agency or provided to it by any third party as required by law.

Data does not include return and return information. "Return" is any tax or information return, declaration of estimated tax; claim for refund; or license, permit, or registration, or other application required by, or provided for or permitted under law and filed with the revenue services commissioner by or on behalf of anyone and any amendment or supplement, including supporting schedules, attachments, or lists.

"Return information" means:

1. a taxpayer's identity;

2. the nature, source, or amount of the taxpayer's income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax collected or withheld, tax underreporting, and overreporting, or tax payments, whether the taxpayer's return was, is being, or will be examined or subjected to other investigation or processing; or

3. other data received by, recorded by, prepared by, furnished to, or collected by the commissioner with respect to a return or to the determination of the existence, or possible existence, of a person's liability for any tax, penalty, interest, fine, forfeiture, or other imposition or offense.

Return information does not include data in a form that cannot be

associated with or otherwise identify, directly or indirectly, a particular taxpayer.

### *Publication of Policies and Procedures*

The bill requires the secretary to establish policies and procedures to:

1. review and respond to queries to ensure that (a) a response is permitted under state and federal law, (b) the privacy and confidentiality of protected data can be assured, and (c) the query is based on sound research design principles, and

2. protect and ensure the security, privacy, confidentiality, and administrative value of data collected and maintained by executive agencies.

### *Information Technology Solution and Data Security Plan*

The secretary must, in consultation with the chief information officer, develop and implement a (1) secure information technology solution to link data across executive agencies and (2) detailed data security and safeguarding plan for the data accessed or shared through such solution.

### *Data-Sharing Memorandum of Understanding*

The secretary must request from, and execute a memorandum of agreement with, each executive agency detailing data-sharing between the agency and OPM. The agreement must authorize OPM to act on behalf of the executive agency that is a party to the agreement for purposes of data access, matching, and sharing, and must include provisions to ensure the proper use, security, and confidentiality of the data shared. Any executive agency the secretary asks to execute such an agreement must comply.

### *Notification Requirements*

The secretary must notify the applicable executive agency when data within the agency's custody has been requested.

### *Labor Commissioner Representative*

Under the bill, OPM is an authorized representative of the labor commissioner or unemployment compensation administrator and must receive, on request, any information in the commissioner's possession relating to employment records that may include (1) an employee's name, Social Security number, and current residential address; (2) employer's name and address and North American Industry Classification System code; and (3) wages.

### *Freedom of Information*

For the purposes of the Freedom of Information Act, OPM must not be considered the agency with custody or control of any public records or files made accessible to the office under the data access program. But OPM must be considered the agency with custody and control of any public records or files it creates, including reports it generates in response to data queries posed under the program.

## BACKGROUND

### *Existing Law's Data Protection Requirements*

The law generally requires anyone who conducts business in Connecticut and who, in the ordinary course of business, owns, licenses, or maintains computerized data that includes personal information to disclose a security breach without unreasonable delay to state residents whose personal information has been, or is reasonably believed to have been, accessed by an unauthorized person. The law requires the person also to provide notice of the security breach to the AG not later than when the affected residents are notified. Failure to provide the notification constitutes a CUTPA violation

The law also specifies that anyone maintaining computerized data that includes personal information he or she does not own must notify the owner or licensee of any breach of the data's security immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized user. The act specifies that this requirement applies only to personal information of

state residents.

The law outlines the notification procedures.

### *CUTPA*

CUTPA prohibits unfair and deceptive acts or practices. It allows the consumer protection commissioner to issue regulations defining what constitutes an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than $5,000, enter into consent agreements, ask the AG to seek injunctive relief, and accept voluntary statements of compliance. It also allows individuals to sue. Courts may issue restraining orders; award actual and punitive damages, costs, and reasonable attorney's fees; and impose civil penalties of up to $5,000 for willful violations and $25,000 for violation of a restraining order.

## COMMITTEE ACTION

Government Administration and Elections Committee

Joint Favorable Substitute
Yea 9 Nay 6 (03/30/2015)